Generative AI in Medical Practice: In-Depth Exploration of Privacy and Security Challenges

Year: 2024 | *Citations: 167* | *Authors: Yan Chen, Pouyan Esmaeilzadeh*

Abstract

As advances in artificial intelligence (AI) continue to transform and revolutionize the field of medicine, understanding the potential uses of generative AI in health care becomes increasingly important. Generative AI, including models such as generative adversarial networks and large language models, shows promise in transforming medical diagnostics, research, treatment planning, and patient care. However, these data-intensive systems pose new threats to protected health information. This Viewpoint paper aims to explore various categories of generative AI in health care, including medical diagnostics, drug discovery, virtual health assistants, medical research, and clinical decision support, while identifying security and privacy threats within each phase of the life cycle of such systems (ie, data collection, model development, and implementation phases). The objectives of this study were to analyze the current state of generative AI in health care, identify opportunities and privacy and security challenges posed by integrating these technologies into existing health care infrastructure, and propose strategies for mitigating security and privacy risks. This study highlights the importance of addressing the security and privacy threats associated with generative AI in health care to ensure the safe and effective use of these systems. The findings of this study can inform the development of future generative AI systems in health care and help health care organizations better understand the potential benefits and risks associated with these systems. By examining the use cases and benefits of generative AI across diverse domains within health care, this paper contributes to theoretical discussions surrounding AI ethics, security vulnerabilities, and data privacy regulations. In addition, this study provides practical insights for stakeholders looking to adopt generative AI solutions within their organizations.